

Date de dépôt : 25 janvier 2017

Réponse du Conseil d'Etat

à la question écrite urgente de M. Jean-Michel Bugnion :
L'utilisation de Google Entreprise par les élèves et les enseignant-e-s de l'école genevoise répond-elle aux normes suisses de protection des données ?

Mesdames et
Messieurs les députés,

En date du 16 décembre 2016, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

Depuis quelque temps le SEM a initié l'implantation de Google Entreprise dans l'école genevoise dans le cadre d'un programme nommé Ecole en ligne (EEL). Les services fournis par Google Enterprise et utilisés par les élèves avec leur compte sont nombreux : e-mail, stockage de données dans un espace privé et un espace partagé, application contacts, agenda, outils de bureautique, Google Photos, navigateur Internet, etc.

A la lumière des recommandations du préposé fédéral à la protection des données et à la transparence (PFPDT) et de la LIPAD, dont quelques extraits figurent ci-dessous, l'implication des services fournis par Google Enterprise, et plus largement les entreprises du numérique, dans l'école genevoise questionne. En effet :

Concernant l'externalisation des données sur un nuage (cloud computing), le PFPDT déconseille fortement cette pratique puisque « les offices fédéraux doivent protéger les citoyens notamment contre les accès non autorisés ». Cette protection n'est en particulier pas possible lorsque le prestataire de service est américain comme Google puisque selon le PFPDT « les autorités américaines peuvent accéder aux données qui sont traitées dans le cadre d'un mandat par des entreprises ayant leur siège aux Etats-Unis. Nous partons de l'idée que les applications en nuage d'entreprises américaines peuvent donc permettre aux autorités américaines d'accéder aux

données clients stockées sur des serveurs dans l'Union européenne ou en Suisse sans avoir à recourir à l'entraide judiciaire internationale, même si une convention complémentaire est prévue ».

Concernant **le webtracking**, le PFPDT nous indique : « nombre des services de webtracking posent problème du point de vue de la protection des données. L'analyse du comportement de navigation permet d'établir des profils de la personnalité au sens de la loi fédérale sur la protection des données. Même le traitement de l'adresse IP d'un internaute relève de la loi fédérale sur la protection des données, puisque cette adresse est par principe à qualifier de donnée personnelle. » Il est de notoriété publique que la plateforme gérée par Google effectue du webtracking.

Concernant **le droit à l'oubli numérique**, le PFPDT déclare : « Le droit à l'oubli numérique peut être défini comme la possibilité de maîtriser ses traces numériques et sa vie (privée et publique) en ligne. » « L'apparition de programmes de recherche et d'analyse toujours plus performants, eux-mêmes combinés à des capacités de stockage quasi illimitées (« Big Data »), conduit à la constatation que l'oubli – dans le sens d'un effacement complet et définitif – sur internet devient souvent illusoire. » Cela étant d'autant plus vrai lorsque le stockage des données est régi par des lois étrangères.

Pour conclure concernant **le cloud computing**, le PFPDT déclare : « La délocalisation de données est toujours risquée. Les 5 risques majeurs sont : 1) perte de contrôle sur les données, 2) manque de séparation et d'isolation des données, 3) non-respect des dispositions légales, 4) accès d'autorités étrangères aux données, 5) captivité des données (le fait de ne pas pouvoir changer aisément de prestataire, par exemple en raisons de spécificités techniques des données traitées incompatibles avec d'autres techniques). »

Quant à la LIPAD, voici ce qu'elle énonce concernant la destruction des données personnelles :

Art. 40 Destruction

¹ Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi.

² Sur décision de l'instance dirigeante de l'institution publique concernée, la destruction de données personnelles peut être différée durant deux ans au maximum à des fins d'évaluation de politiques publiques. Ces données sont dès lors soustraites à communication, sauf si elles sont accessibles au regard de la loi sur les archives publiques, du 1^{er} décembre 2000, ou du titre II de la présente loi.

Concernant la sécurité des données :

Art. 37 Sécurité des données personnelles

¹ Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

² Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter.

³ Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.

À la lecture des recommandations du PFPDT et de la LIPAD, l'implantation de Google Entreprise dans l'école genevoise m'apparaît comme fort préoccupante et m'amène à poser les questions suivantes :

- **L'utilisation des services de Google Entreprise dans le cadre de la plateforme EEL respecte-elle les recommandations du PFPDT telles que rapportées ci-dessus ?**
- **L'utilisation des services de Google Entreprise dans le cadre de la plateforme EEL respecte-elle la LIPAD ?**
- **Un consentement est-il demandé aux parents des élèves et aux enseignant-e-s avant la création des comptes chez Google ?**
- **L'anonymisation des identifiants des élèves pour masquer l'identité des personnes est-elle efficace ? Peinez-vous à reconnaître francois.lngchmp ou antonio.hdgrs ? (Ces deux exemples ont été anonymisés selon le même principe que celui utilisé pour les élèves).**
- **Qu'en est-il de la responsabilité légale des mineurs lors de l'utilisation des services de Google Entreprise ?**
- **Qu'en est-il de la responsabilité légale des enseignant-e-s lors de l'utilisation des services de Google Entreprise par eux ou leurs élèves ?**
- **L'acceptation des conditions générales de Google Entreprise par un élève est-elle suffisante et conforme aux yeux de la loi ?**
- **Dans quelle mesure l'utilisation de Google Entreprise est-elle imposée aux enseignant-e-s ?**

Devant l'importance des enjeux au niveau de la protection des données de nos élèves, pour la plupart mineurs, ainsi que du corps enseignant que représente cette problématique de l'implication des entreprises du numérique dans l'école, et en particulier celle d'une major du Web telle que Google soumise à la législation américaine, je remercie le Conseil d'Etat de ses futures réponses que je souhaite développées et rassurantes.

RÉPONSE DU CONSEIL D'ÉTAT

Il convient tout d'abord de rappeler qu'en matière de protection des données, l'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD – A 2 08) et de son règlement d'application, du 21 décembre 2011 (RIPAD – A 2 08.01) est *alternative* à celle de la loi fédérale sur la protection des données personnelles, du 19 juin 1992 (LPD – rs/CH 235.1). Dans la mesure où les rapports de droit liant l'école publique genevoise et ses élèves entrent pleinement dans le champ d'application de la LIPAD, les avis du préposé fédéral à la protection des données et à la transparence (PFPDT) et les dispositions de la LPD ne sont pas contraignants pour l'administration cantonale et le département de l'instruction publique, de la culture et du sport (DIP) en particulier.

L'utilisation de la suite logicielle en ligne *Google Apps* a été testée dans le cadre pédagogique au DIP dès 2011. En 2014, l'accord a été donné pour une extension progressive et cadrée de la solution aux écoles des degrés secondaires.

La plateforme utilisée est une variante de *Google Apps Entreprise* destinée spécifiquement à l'éducation, dont les caractéristiques et conditions d'utilisation sont déterminées contractuellement.

Ainsi, l'instance utilisée est uniquement visible et disponible pour les utilisateurs que le DIP autorise. Il est par exemple impossible à un élève de partager un document avec une personne externe à l'institution scolaire. Les droits d'administrateurs sont exercés par le DIP, lequel peut créer ou supprimer les accès, autoriser ou non telle ou telle fonction pour un groupe d'utilisateurs et exercer un contrôle sur l'usage qui est fait de la plateforme.

Pour sa part, Google s'engage à ne diffuser aucune publicité dans les outils de la suite logicielle (messagerie, moteur de recherche, etc.) et à ne pas collecter les données des élèves pour réaliser des profils d'annonces. Le « webtracking » qui est réalisé pour les versions publiques des outils de Google est donc désactivé dans la version mise à disposition des institutions

scolaires. Par ailleurs, Google précise que les données stockées dans les versions entreprises et éducation de sa suite appartiennent intégralement à ses clients et que la société se fait un devoir impératif d'en protéger la confidentialité, sous réserve des dispositions impératives du Data Privacy Act qui l'obligeraient à communiquer ces données au gouvernement des Etats-Unis. La société s'engage également à effacer totalement les données de ses serveurs dans les 6 mois à compter de la date à laquelle elles auront été supprimées par un utilisateur.

Une analyse des risques liés à l'introduction de *Google Apps* dans le système d'information pédagogique a été menée. Les recommandations issues de cette analyse ont abouti à la mise en place d'une politique de sensibilisation, de prescriptions d'usage des outils et de contrôles destinés à renforcer la protection des données.

L'utilisation de Google avec un annuaire des utilisateurs maîtrisé par l'Etat permet de ne transmettre à la société de service pour la création des comptes que les données strictement nécessaires et aucune donnée personnelle d'élèves, puisque les identifiants de ces derniers sont des pseudonymes. Cette façon de faire permet certes à une personne qui connaît le nom de l'élève de reconnaître son identifiant, mais elle ne permet pas à un tiers d'établir aisément une correspondance automatique entre une personne et son identifiant. Ce procédé avait été soumis en 2012 au Préposé cantonal à la protection des données et à la transparence (PPDT) et à la direction des affaires juridiques du DIP qui l'avaient jugé nécessaire et suffisant pour être compatible avec la LIPAD. A noter que l'annuaire « Ecole en ligne » n'est pas utilisé pour accéder uniquement à *Google Apps*, mais également à de nombreux autres services hébergés au sein de l'Etat, ou à des plateformes externes validées par le DIP.

Autre mesure : l'utilisation de la plateforme Google à des fins administratives n'est pas autorisée. Par ailleurs, les utilisateurs sont informés qu'aucune donnée personnelle – et encore moins une donnée sensible – ne doit être déposée sur *Google Apps*. Ceci figure dans la directive départementale « Condition d'utilisation des outils et services informatiques destinés à la pédagogie »¹ et est rappelé à chaque enseignant et chaque élève lors de la validation de son compte.

Comme pour d'autres services utilisés par les écoles, les élèves et leurs représentants légaux sont informés, en début d'année scolaire, des outils mis à disposition et de leurs règles d'utilisation, soit via le memento de l'établissement, soit via une circulaire à signer. L'activation du compte

¹ <http://icp.ge.ch/dip/refdip/spip.php?article388>

« Ecole en ligne » est normalement réalisée lors des cours de technologies de l'information et de la communication (TIC) en première année du cycle d'orientation et des explications circonstanciées sont fournies aux élèves dans ce cadre.

Pour ce faire, le service écoles-médias (SEM) a entrepris de nombreuses actions de sensibilisation à la protection des données à l'attention des enseignants et, à travers eux, des élèves. Depuis la fin 2016, le SEM est aussi intervenu directement auprès des élèves – du centre de formation professionnelle construction (CFPC) dans un premiers temps – pour une sensibilisation aux risques des technologies numériques concernant la protection de la vie privée et des données personnelles.

Enfin, le Conseil d'Etat n'entend pas donner à l'usage de Google une position exclusive. C'est la raison pour laquelle plusieurs plateformes collaboratives sont proposées aux écoles et aux enseignants, permettant un usage différencié et complémentaire de chacune d'entre elles².

Ceci étant précisé, il importe de reconnaître que la LIPAD vise aussi la confidentialité vis-à-vis de Google, gestionnaire de la plate-forme, et pas seulement des autres tiers. Or, Google a techniquement la possibilité d'accéder aux données déposées sur sa plate-forme, au même titre que l'administrateur du DIP. Seuls ses engagements contractuels l'en empêchent, mais l'Etat de Genève n'a aucun moyen de vérifier le respect par Google de ses engagements. Trois éléments doivent ici être apportés au débat :

- La loi sur l'administration en ligne (LAeL – B 4 23) a été adoptée récemment par le Grand Conseil³. Elle prévoit une revue périodique des mesures de sécurité mises en œuvre pour assurer la confidentialité des données à caractère personnel, assurant une amélioration constante des solutions retenues. Or l'usage fait par le DIP de Google Apps for Education entre dans le champ d'application de cette loi.
- Un projet de modification du RIPAD est à l'étude. Il vise à rendre ce règlement plus conforme à la réalité technique de l'Internet, en matière notamment de communication transfrontière des données. Ce projet prévoit l'ajout d'un article 13A dont la teneur est la suivante :

Art. 13A Sous-traitance (art. 37, al. 2, de la loi) (nouveau)

¹ Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

² <http://edu.ge.ch/sem/node/275>

³ Loi 11684, du 23 septembre 2016, dont l'entrée en vigueur reste à fixer.

² *L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.*

³ *La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.*

⁴ *Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.*

⁵ *S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.*

⁶ *Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.*

- La Suisse a conclu ce 11 janvier un accord « Bouclier de protection des données Suisse-Etats-Unis », calqué sur l'accord passé entre les Etats-Unis et l'Union européenne. Il vise à remplacer le « Safe Harbour » dénoncé par l'Union européenne. En vertu de ce nouvel accord, et moyennant respect des mesures préconisées par ce dernier, les Etats-Unis sont considérés par le PFPDT comme assurant un niveau de protection adéquat au sens de l'article 7 de l'ordonnance fédérale relative à la loi fédérale sur la protection des données, du 14 juin 1993 (OLPD – rs/CH 235.11)⁴.

A l'aune de ces trois changements, le recours à *Google Apps for Education* constitue une sous-traitance qui pourra être conforme au futur article 13A RIPAD, lui-même conforme à la LIPAD, à condition de respecter les exigences contractuelles prescrites par son alinéa 3. On remarquera que cette disposition est plus exigeante que celle de la LPD, puisqu'il n'est pas possible de réparer par une convention privée passée avec le sous-traitant le caractère inadéquat de la législation étrangère qui lui serait applicable.

⁴ <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-65210.html>

La solution adoptée, si elle n'est pas parfaite, l'a enfin été en considération d'éléments économiques. L'utilisation de *Google Apps for Education*, gratuite pour les institutions scolaires, permet ainsi de doter chaque élève d'une boîte aux lettres institutionnelle (mais également d'un espace de stockage de documents et d'outils collaboratifs performants). Il serait à terme possible de mettre une solution permettant au DIP de s'affranchir des services de Google pour la messagerie des élèves, mais il demeure qu'un budget spécifique devrait être alloué à ce projet. Au-delà de ces éléments économiques, l'usage clairement cadré de Google dans le cadre scolaire permet également à l'école de remplir sa mission éducative, en sensibilisant les élèves aux risques des technologies et à la protection de leurs données personnelles. Ces derniers seront ainsi mieux préparés à l'usage d'outils qui, dans la vie privée et professionnelle, sont devenus incontournables.

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :
Anja WYDEN GUELPA

Le président :
François LONGCHAMP